CLAIMS

Having thus described our invention, what we claim as new, and desire to secure by Letters Patent is:

1. A method for securely handling an information unit by a first information processing device (2) interoperating with a second secure information processing device (1), in particular a chip card, whereby the information unit is provided by an issuer,

the method comprising the steps:

providing (3, 25, 35) the information unit from the issuer to the first information processing device (2), the information unit being processed by a cryptographic process;

providing at least one key for the cryptographic process on the second secure information processing device (1); and

cryptographically reprocessing (29, 38) the information unit by using the at least one key.

2. The method according to claim 1, comprising:

providing (3, 25, 35) the information unit from the issuer to the first information processing device (2), the information unit being encrypted by using at least a first key;

providing the first key from the issuer to the first information processing device (2), the first key being encrypted by using at least a second key;

providing the at least one second key on the second secure information processing device (1);

interconnecting the first information processing device (2) and the second secure information processing device (1);

on side of the second secure information processing device, decrypting (27) the at least first key by using the at least second key; and

decrypting (29) the information unit by using the decrypted at least first key.

3. The method according to claim 1, comprising:

providing (3, 25, 35) the information unit from the issuer to the first information processing device (2), the information unit being signed by using a signature;

providing the signature from the issuer to the first information processing device (2), the signature being generated by using at least one key;

providing the at least one key for signature verification on the second secure information processing device (1);

interconnecting the first information processing device (2) and the second secure information processing device (1);

transferring the at least one key for signature verification from the second secure information processing device to the first information processing device; and

verifying the signature of the information unit by using the at least one key.

4. The method according to claim 2, wherein the decrypted at least first key is transferred to the first information processing device (2) and the information unit is decrypted (29) on side of the first device (2).

5. The method according to claim 1, wherein the first information processing device (2) provides a control command (26, 36) to the second secure information processing device (1) to initiate decryption of the at least first key by using the at least second key and/or to initiate transferring the signature key for signature verification from the second secure device to the first device.

6. The method according to claim 5, wherein the encrypted information unit, the encrypted first key, and/or the signature key, and/or the generated signature, and/or the control command are downloaded (25, 35) from a central server (4).

7. The method according to claim 3, wherein the second key and/or the key for signature verification are/is securely stored on the second secure device (1) at time of its issuing by the issuer.

8. The method according to claim 2, wherein at least a third key is provided for external authentication and/or release control of the respective information unit.

9. The method according to claim 8, wherein the first device (2) is initiated to gather a new release of the information unit from the issuer, depending on the respective status of the third key.

10. The method according to claim 9, wherein the new release of the information unit is downloaded from an internet server (4) provided by the issuer.

11. The method according to claim 2, wherein the at least first key and/or the signature are/is randomized between different sessions of

providing the information unit from the issuer to the first device (2).

12. The method according to claim 1, wherein the first information processing device (2) is a terminal device, and the second secure information processing device (1) is a portable device.

13. The method according to claim 12, wherein the terminal device is a chip card reader and the portable device is a chip card.

14. A system for securely handling an information unit, comprising a first information processing device (2) interoperating with a second secure information processing device (1), in particular a chip card, the information unit being provided by an issuer,

comprising:

the first device (2) comprising
a storage for storing the information unit; and

the second secure device (1) comprising
a storage (6) for storing at least one key for a cryptographic process; and

providing means for cryptographically reprocessing the information unit by using the at least one key.

15. The system according to claim 14, wherein

the first device (2) comprises
a storage for storing the information unit, encrypted by using at least a first key, and a storage for storing the first key, encrypted by using at least a second key;

the second secure device (1) comprises
a storage (6) for storing the at least one second key, and processing means for decrypting the at least first key by using the at least second key; and

providing means for decrypting the information unit by using the decrypted at least first key.

16. The system according to claim 14, wherein

the first device (2) comprises
a storage for storing the information unit and a signature for the information unit;

the second secure device (1) comprises
a storage (6) for storing at least one signature key;

providing means for verifying the signature of the information unit by using the at least one signature key.

17. The system according to claim 14, wherein the second secure device (1) provides an access control by means of the information unit.

18. The system according to claim 14, wherein the second secure device (1) comprises a processor to make specific functions of the second secure device usable/accessible on the first device or on at least a third device (5) attached to the first device.

19. The system according to claim 14, wherein the first device (2) comprises processing means for decrypting (29) the information unit by use of the decrypted at least first key.

20. The system according to claim 14, wherein the second secure device (1) comprises means to initiate decryption of the at least first key by using the at least second key and/or means to initiate transfer of the signature key for signature verification from the second secure device to the first device.

21. The system according to claim 14, wherein the first device (2) comprises means to download the encrypted information unit, the encrypted first key, and/or the generated signature,

and/or the control command, from a central server (4).

22. The system according to claim 14, wherein the second secure device (1) comprises a non-erasable storage to store the second key and/or the signature key at time of its issuing.

23. The system according to claim 14, wherein the first device (2) and/or the second secure device (1) comprise/s a storage (6) for storing at least a third key for external authentication and/or release control of the information unit and processing means (7) for processing the third key.

24. The system according to claim 23, wherein the first device (2) comprises means to initiate download of a new release of the information unit, depending on the respective status of the third key.

25. The system according to claim 21, wherein the central server (4) comprises a randomizer for randomizing the at least first key and/or the signature between different sessions of providing the information unit from the issuer to the first device.

26. The system according to claim 14, wherein the first information processing device (2) is a terminal device and the second secure

information processing device (1) is a portable device.

27. The system according to claim 26, wherein the terminal device is a chip card reader and the portable device is a chip card.

28. A chip card (1) for securely handling an information unit by interoperating with an information handling terminal device (2), comprising a storage (6) for storing an at least one key for the cryptographic process.

29. The chip card according to claim 28, wherein processing means (7) performing an access control is controlled by an information unit.

30. The chip card according to claim 28, wherein a processor (7) runs specific functions on the terminal device (2, 5) or on at least a second device attached to the terminal device (2, 5).

31. The chip card according to claim 28, further comprising means for transferring of the at least one second key to the terminal device (2, 5) and/or means for decrypting of the at least first key by using the at least second key and/or means to initiate transfer of the signature key for signature verification.

32. The chip card according to claim 30, wherein a non-erasable storage (6) stores the second key and/or the signature key at time of its issuing.

33. The chip card according to claim 32, further comprising a storage (6) for storing at least a third key for external authentication and/or release control of the information unit and processing means (7) for processing the third key.

34. The chip card according to claim 33, wherein said processing means (7) initiates download of a new release of the information unit, depending on the respective status of the third key.

35. A chip card accepting device (2), in particular a chip card reader, for securely handling an information unit by interoperating with a chip card (1), comprising a storage for storing the information unit.

36. The chip card accepting device according to claim 35, further comprising means for decrypting the information unit by using at least one key.

37. The chip card accepting device according to claim 36, further comprising means for verifying a digital signature.

38. The chip card accepting device according to claim 37, further comprising means for downloading the encrypted information unit, the at least one key and the digital signature from a central server (4).

39. The chip card accepting device according to claim 35, further comprising a storage for storing at least a third key for external authentication and/or release control of the information unit and processing means for processing the third key.

40. The chip card accepting device according to claim 39, further comprising means to initiate download of a new release of the information unit, depending on the respective status of the third key.